

Table 4: Description of the malware used in the test

Malware name *	Executable files of malware	Comments
Trojan-Spy.Win32.Goldun.hn	\SystemRoot\system32\hpprintdrv.sys \SystemRoot\system32\hpprintx.dll	Hidden all PE-files
Trojan-Proxy.Win32.Wopla.ag	\SystemRoot\system32\poof \SystemRoot\system32\koos.exe \SystemRoot\system32\kprof	Hidden all PE-files, koos.exe process, poof-driver in the memory and autorun registry key
SpamTool.Win32.Mailbot.bd	\SystemRoot\System32:18467	Hidden file, process, driver and autorun registry key
Monitor.Win32.EliteKeylogger.21	\SystemRoot\system32\packasvr.exe \SystemRoot\system32\drivers\usbex.sys \SystemRoot\system32\drivers\isapnp2k.sys \SystemRoot\system32\drivers\mupnt.sys \SystemRoot\system32\stccache.dll \SystemRoot\system32\mtx32.dll	Hidden all PE-files, process, driver and autorun registry key
Rootkit.Win32.Agent.ea	\SystemRoot\system32\drivers\Lsw61.sys	Hidden file and autorun registry key
Rootkit.Win32.Podnuha.a**	\SystemRoot\system32\drivers\iefjuojs.sys \SystemRoot\system32\system32\aicaaic.dll	Locked iefjuojs.sys file, also locked deleting/modification of the autorun registry keys and aicaaic.dll file. In testing on this rootkit we take into account only detection and deleting iefjuojs.sys, because aicaaic.dll isn't hidden or locked.

Table 5: Description of proof-of-concept rootkits used in the test

Proof-of-concept rootkit	Comments
Unreal A (v1.0.1.0)	Hidden file C:\:unreal.sys and driver in the memory
RkDemo v1.2	Hidden process RKSTART.EXE
FuTo	Hidden process with defined PID
HideToolz	Hidden process HideToolz.exe

* - malware names are specified in accordance with the Kaspersky Lab classification

Table 6: Malware disguise method (intercepted API)

Malware name *	Disguise method (intercepted API)
Trojan-Spy.Win32.Goldun.hn	UserMode (function code modification) ntdll.dll:LdrLoadDll wininet.dll:InternetConnectA KernelMode (addresses editing in KiST) NtCreateProcess NtCreateProcessEx NtQueryDirectoryFile
Trojan-Proxy.Win32.Wopla.ag	KernelMode (splicing) NtCreateFile NtCreateKey NtEnumerateKey NtEnumerateValueKey NtOpenFile NtOpenKey NtQueryDirectoryFile NtTerminateProcess DKOM
SpamTool.Win32.Mailbot.bd	Ntfs IRP_MJ_CREATE Ntfs IRP_MJ_QUERY_INFORMATION IDT[2E] SYSENTER DKOM
Monitor.Win32.EliteKeylogger.21	KernelMode (addresses editing in KiST) NtCreateKey NtEnumerateKey NtOpenKey Driver-filter
Rootkit.Win32.Agent.ea	KernelMode (splicing) NtEnumerateKey NtOpenKey Ntfs IRP_MJ_CREATE Ntfs IRP_MJ_DIRECTORY_CONTROL
Rootkit.Win32.Podnuha.a	KernelMode (splicing) ObOpenObjectByName

Table 7: Disguise method of proof-of-concept rootkits (intercepted API)

Proof-of-concept rootkit	Disguise method (intercepted API)
Unreal A (v1.0.1.0)	DKOM Driver-filter
RkDemo v1.2	DKOM
FuTo	DKOM
HideToolz	KernelMode (addresses editing in KiST) NtClose NtDuplicateObject NtInitiatePowerAction NtMapViewOfSection NtOpenProcess NtOpenThread NtQueryInformationProcess NtQuerySystemInformation NtRaiseHardError NtResumeThread NtSetInformationThread NtSetSystemPowerState NtShutdownSystem NtTerminateProcess NtWriteFile NtWriteFileGather

* - malware names are specified in accordance with the Kaspersky Lab classification

Table 7: Malware names in classifications of leading antivirus vendors

Kaspersky Lab	Symantec	McAfee	DrWeb
Trojan-Proxy.Win32.Wopla.ag	Trojan.Dropper	Generic.dx	Trojan.Sklog
Rootkit.Win32.Agent.ea	Trojan.Srizbi	Generic.dx	Trojan.Spambot
Trojan-Spy.Win32.Goldun.hn	Trojan.Goldun	PWS-Goldun.dr	Trojan.PWS.GoldSpy
SpamTool.Win32.Mailbot.bd	Backdoor.Rustock.A	Spam-Mailbot.c	Trojan.MulDrop.3785
Rootkit.Win32.Podnuha.a	Trojan Horse	Generic.dx	Trojan.PWS.GoldSpy
Monitor.Win32.EliteKeylogger.21	Spyware.EliteKeylogger	Keylog-Elt	Program.EliteKeylogger.36